Privacy, Security and facial deidentification aspects

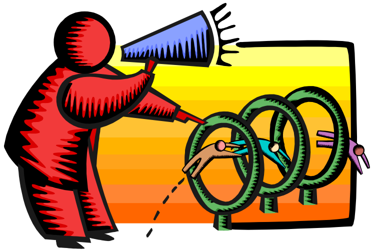
By

Mickey Cohen, CEO

Shanit Ltd

Mickey@shanit.co.il

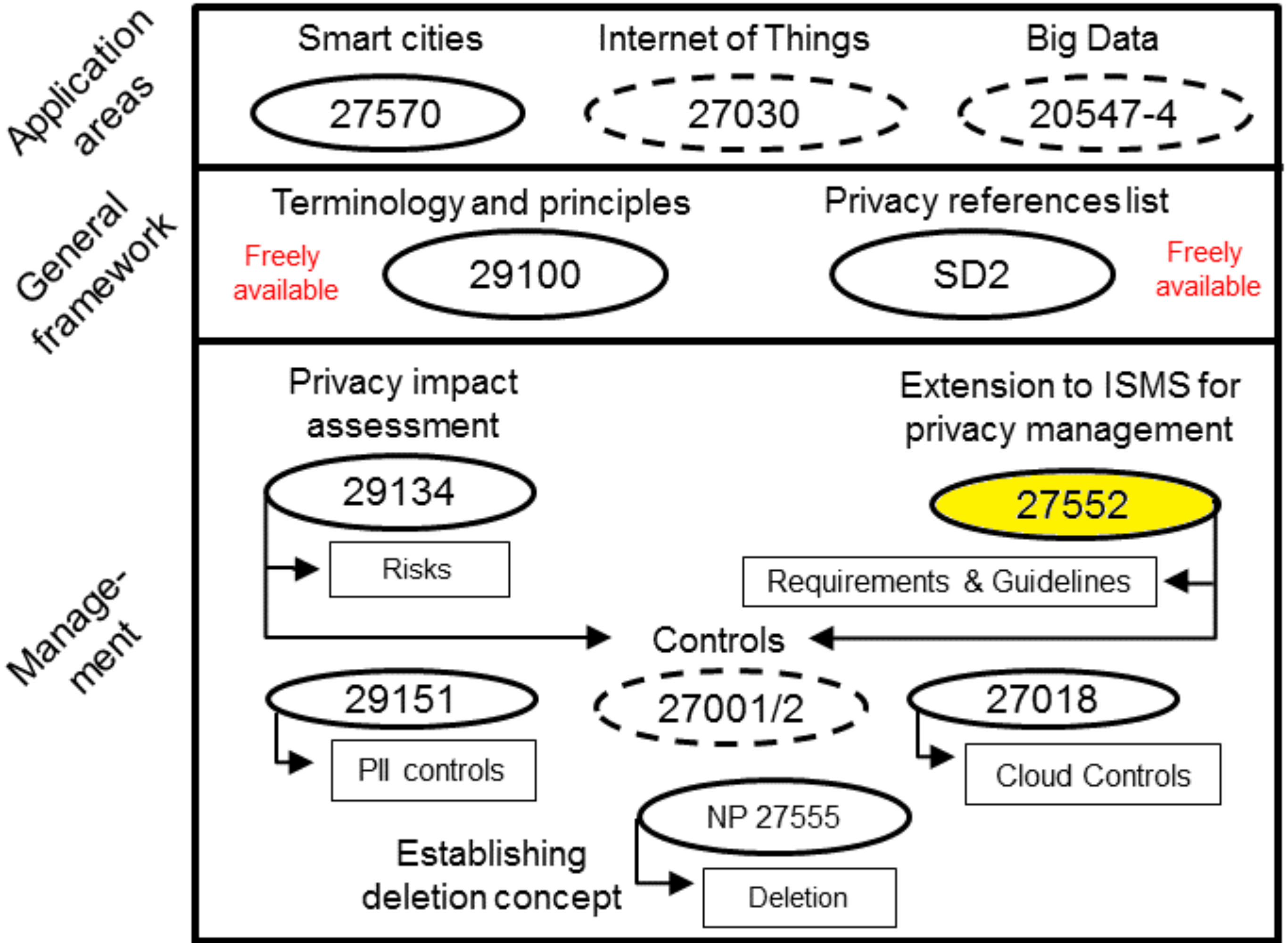
+972-54-758-6312



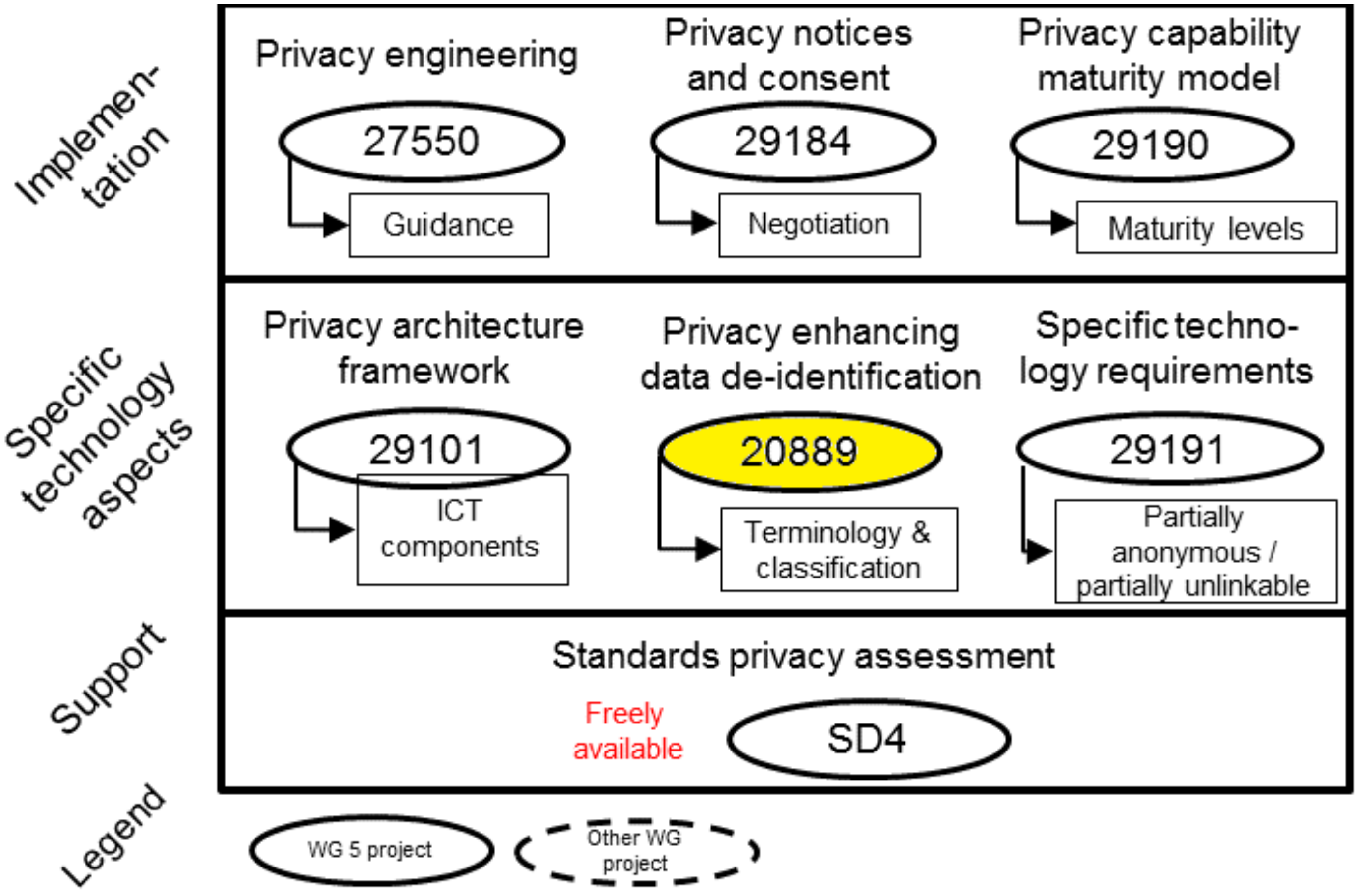
Presentation layout

- SC27/WG5 Identity management and privacy technologies (ISO/IEC 20889, 27552)
- SC27 IT Security techniques (ISO 27xxx)
- Practical workflows and privacy
- Examples
- Summary

ISO 27552 - Extension to ISO/IEC 27001 and **ISO/IEC 27002** for privacy information management — Requirements and guidelines



ISO 20899 - Privacy enhancing data **de-identification** terminology and classification of techniques



Implementation

Privacy engineering

27550

Guidance

Privacy notices and consent

29184

Negotiation

Privacy capability maturity model

29190

Maturity levels

Specific technology aspects

Privacy architecture framework

29101

ICT components

Privacy enhancing data de-identification

20889

Terminology & classification

Specific technology requirements

29191

Partially anonymous / partially unlinkable

Support

Standards privacy assessment

Freely available

SD4

Legend

WG 5 project

Other WG project

Privacy and Security

- ISO/IEC 27522 maps Privacy Information Management System (PIMS) onto Information Security Management System (ISMS) so that Personally Identifiable Information (PII) can be addressed through a known framework.
- Security is a moving balance between Requirements, Threats, Usability and … Budgets.

ISO/IEC 27522

- Guidance for Privacy by Design (PdD)
- Limitations on collection, on processing, minimization, de-identification, deletion, end of processing, retention, disposal etc.
- Transfer and record of transfer of PII
- Addresses Controllers and Processors
- Relates closely with General Data Protection Regulation (GDPR)

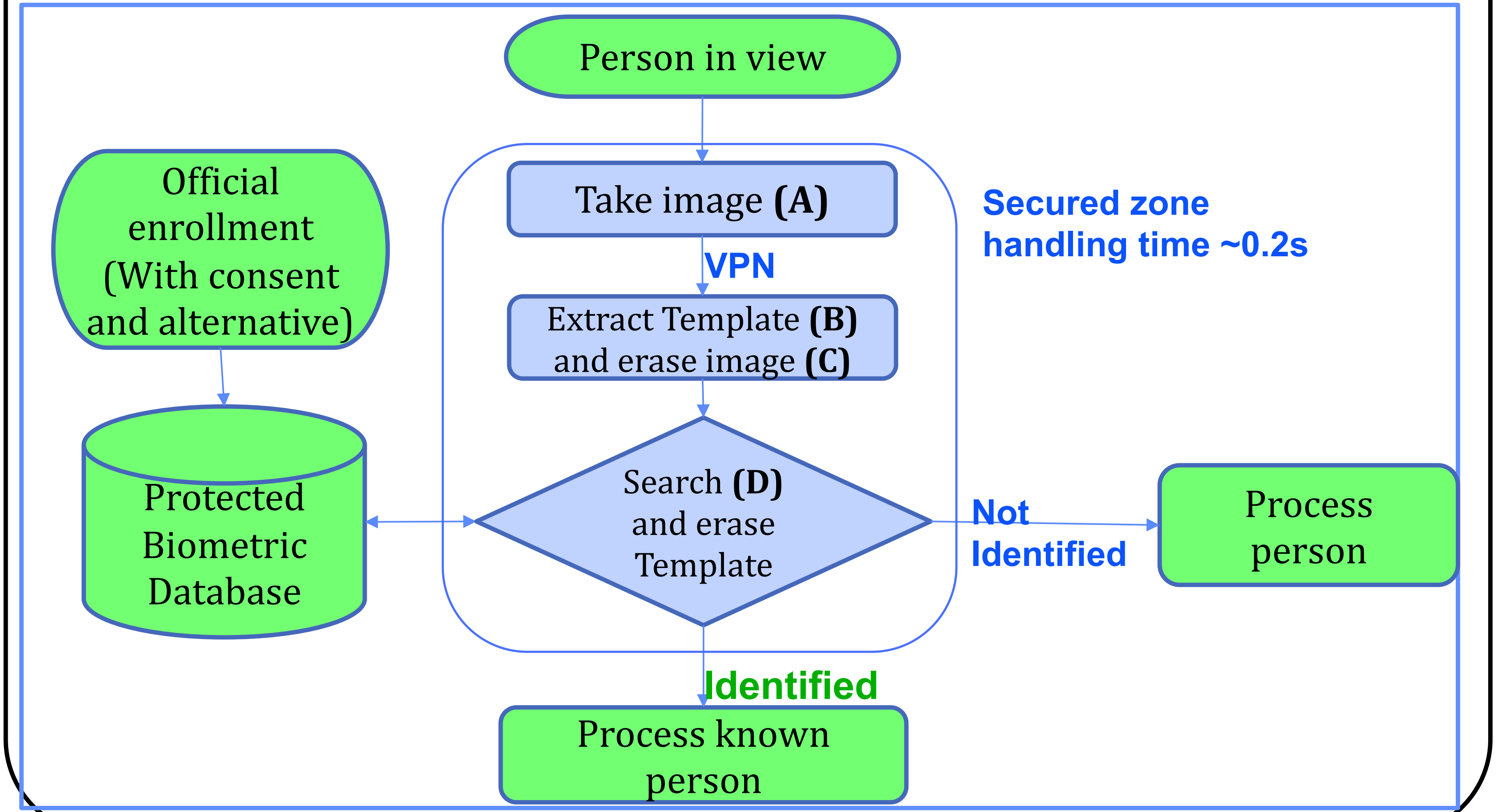
ISO/IEC 20889 De-Identification

- Addresses de-identification of PII by removal of any possible link with a data subject (natural person) GDPR, HIPPA, COPA etc.
- Addresses risks of re-identification attacks
- Discusses de-identification techniques
- Addresses anonymization, pseudonymisation
- Suggests techniques such as noise, permutations, encryption, synthetic data
- Formal privacy measurement models

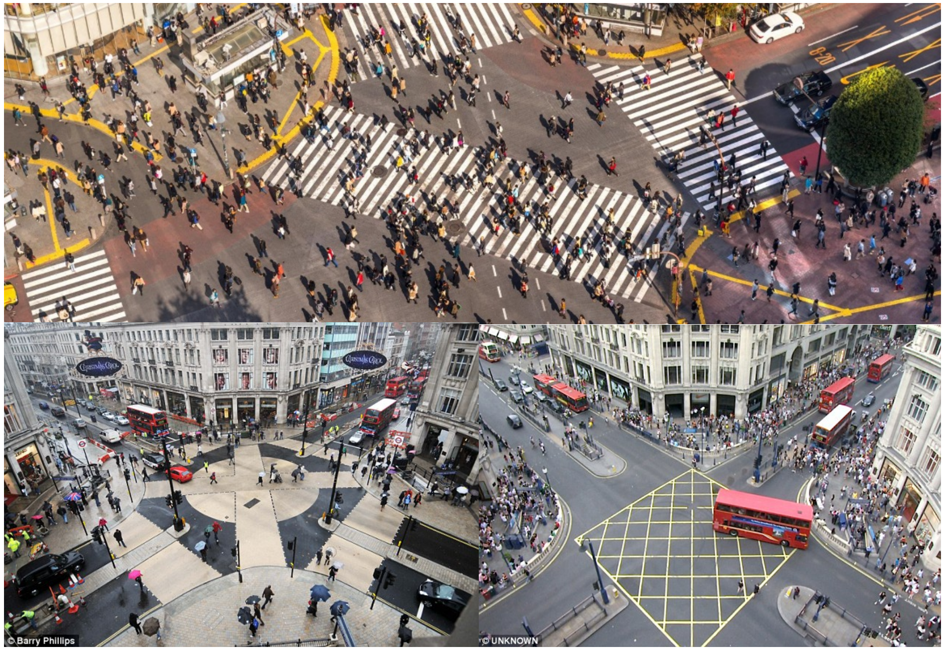
ISO/IEC 20889 De-Identification

No practical implementation or tool for de-identification is suggested

Privacy Risk over exposure time


Person in view
Take image **(A)**
VPN
Extract Template **(B)** and erase image **(C)**
Search **(D)** and erase Template
Official enrollment (With consent and alternative)
Protected Biometric Database
Secured zone handling time ~0.2s
Not Identified
Process person
Identified
Process known person

Privacy Risk and search space



© Barry Phillips

© UNKNOWN

- Images – more like bolbs
- “Search space” 100 people
- Images kept for 20-30 seconds
- No real risk of identification

Is there a quality level below which privacy is a lesser issue? Is time a factor ?

De-Identification

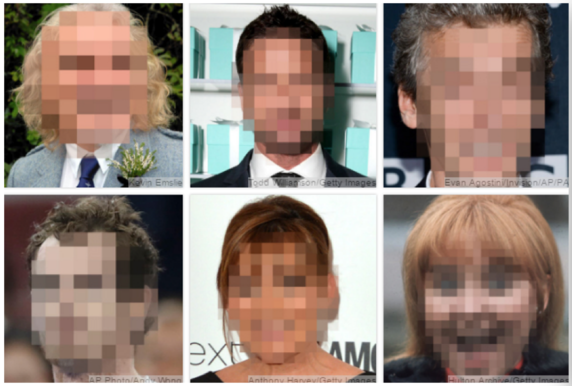
- Every database is destined to be breached.
- Many organizations need to keep facial images
- Many organization have facial images pending consent

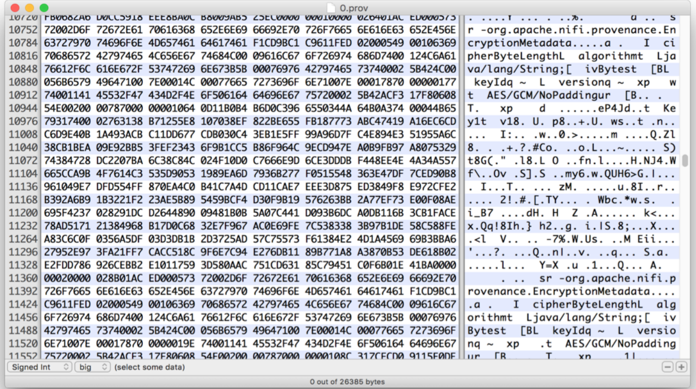
De-Identification - Solution

- Process images so that they are similar to humans and resist Face Recognition Technologies .
- Images displayed to officers or printed are only the De-Identified version

De-Identification - Traditional

D-ID
Firewall for your identity.


Kevin Emslie
Todd Williamson/Getty Images
Evan Agostini/Invision/AP/PA
AP Photo/Andy Wong
Anthony Harvey/Getty Images
Hulton Archive/Getty Images

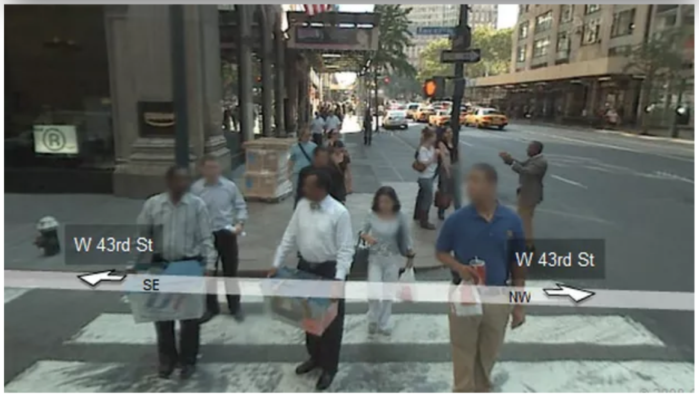


```
10720 FB0682A6 D0CC5918 EEE8BA0C B8009AB5 25EC0000 00010000 026401AC ED000573  . ....Y ... . ..%.          d ..  s
10752 72002D6F 72672E61 70616368 652E6E69 66692E70 726F7665 6E616E63 652E456E  r -org.apache.nifi.provenance.En
10784 63727970 74696F6E 4D657461 64617461 F1CD9BC1 C9611FED 02000549 00106369  cryptionMetadata.....a .   I  ci
10816 70686572 42797465 4C656E67 74684C00 09616C67 6F726974 686D7400 124C6A61  pherByteLengthL  algorithmt  Lja
10848 76612F6C 616E672F 53747269 6E673B5B 00076976 42797465 73740002 5B424C00  va/lang/String;[  ivBytest  [BL
10880 056B6579 49647100 7E00014C 00077665 7273696F 6E71007E 00017870 00000177   keyIdq ~  L  versionq ~  xp   w
10912 74001141 45532F47 434D2F4E 6F506164 64696E67 75720002 5B42ACF3 17F80608  t  AES/GCM/NoPaddingur  [B.. .
10944 54E00200 00787000 00001064 0D11B0B4 B6D0C396 6550344A 64B0A374 00044B65  T.   xp     d  ......eP4Jd..t  Ke
10976 79317400 02763138 B71255E8 107038EF 822BE655 FB187773 ABC47419 A16EC6CD  y1t  v18. U. p8..+.U. ws..t .n..
11008 C6D9E40B 1A493ACB C11DD677 CDB030C4 3EB1E5FF 99A96D7F C4E894E3 51955A6C  ...  I:.. .w..0.>.....m ....Q.Zl
11040 38CB1BEA 09E92BB5 3FEF2343 6F9B1CC5 B86F964C 9ECD947E A0B9FB97 A8075329  8. .  .+.?.#Co. ..o.L...~..... S)
11072 74384728 DC2207BA 6C38C84C 024F10D0 C7666E9D 6CE3DDDB F448EE4E 4A34A557  t8G(." .l8.L O ..fn.l....H.NJ4.W
11104 665CCA9B 4F7614C3 535D9053 1989EA6D 7936B277 F0515548 363E47DF 7CED90B8  f\..Ov .S].S ..my6.w.QUH6>G.|...
11136 961049E7 DFD554FF 870EA4C0 B41C7A4D CD11CAE7 EEE3D875 ED3849F8 E972CFE2  . I...T.. ... zM. .....u.8I..r..
11168 B392A6B9 1B3221F2 23AE5B89 5459BCF4 D30F9B19 576263BB 2A77EF73 E00F08AE  .... 2!.#.[.TY... . Wbc.*w.s.  .
11200 695F4237 028291DC D2644890 09481B0B 5A07C441 D093B6DC A0DB116B 3CB1FACE  i_B7 ....dH. H  Z .A...... k<...
11232 78AD5171 21384968 B17D0C68 32E7F967 AC0E69FE 7C538338 3B97B1DE 58C588FE  x.Qq!8Ih.} h2..g. i.|S.8;...X...
11264 A83C6C0F 0356A5DF 03D3DB1B 2D3725AD 57C75573 F61384E2 4D1A4569 69B3BBA6  .<l  V.. .. -7%.W.Us. ..M Eii...
11296 27952E97 3FA21FF7 CACC518C 9F6E7C94 E276DB11 89B771A8 A3870B53 DE618B02  '...?. ...Q..n|..v. ..q... S.a.
11328 E2FDD786 926CEBB2 E1011759 3D580AAC 751CD631 85C79451 C0F6B01E 41BA0000  .....l...  Y=X .u .1...Q... A.
11360 00020000 028B01AC ED000573 72002D6F 72672E61 70616368 652E6E69 66692E70      . ..  sr -org.apache.nifi.p
11392 726F7665 6E616E63 652E456E 63727970 74696F6E 4D657461 64617461 F1CD9BC1  rovenance.EncryptionMetadata....
11424 C9611FED 02000549 00106369 70686572 42797465 4C656E67 74684C00 09616C67  .a .   I  cipherByteLengthL  alg
11456 6F726974 686D7400 124C6A61 76612F6C 616E672F 53747269 6E673B5B 00076976  orithmt  Ljava/lang/String;[  iv
11488 42797465 73740002 5B424C00 056B6579 49647100 7E00014C 00077665 7273696F  Bytest  [BL  keyIdq ~  L  versio
11520 6E71007E 00017870 0000019E 74001141 45532F47 434D2F4E 6F506164 64696E67  nq ~  xp   .t  AES/GCM/NoPadding
11552 75720002 5B42ACF3 17F80608 54F00200 00787000 0000108C 317CFCD0 9115F0DF  ur  [B.  .  T   xp    1|
```

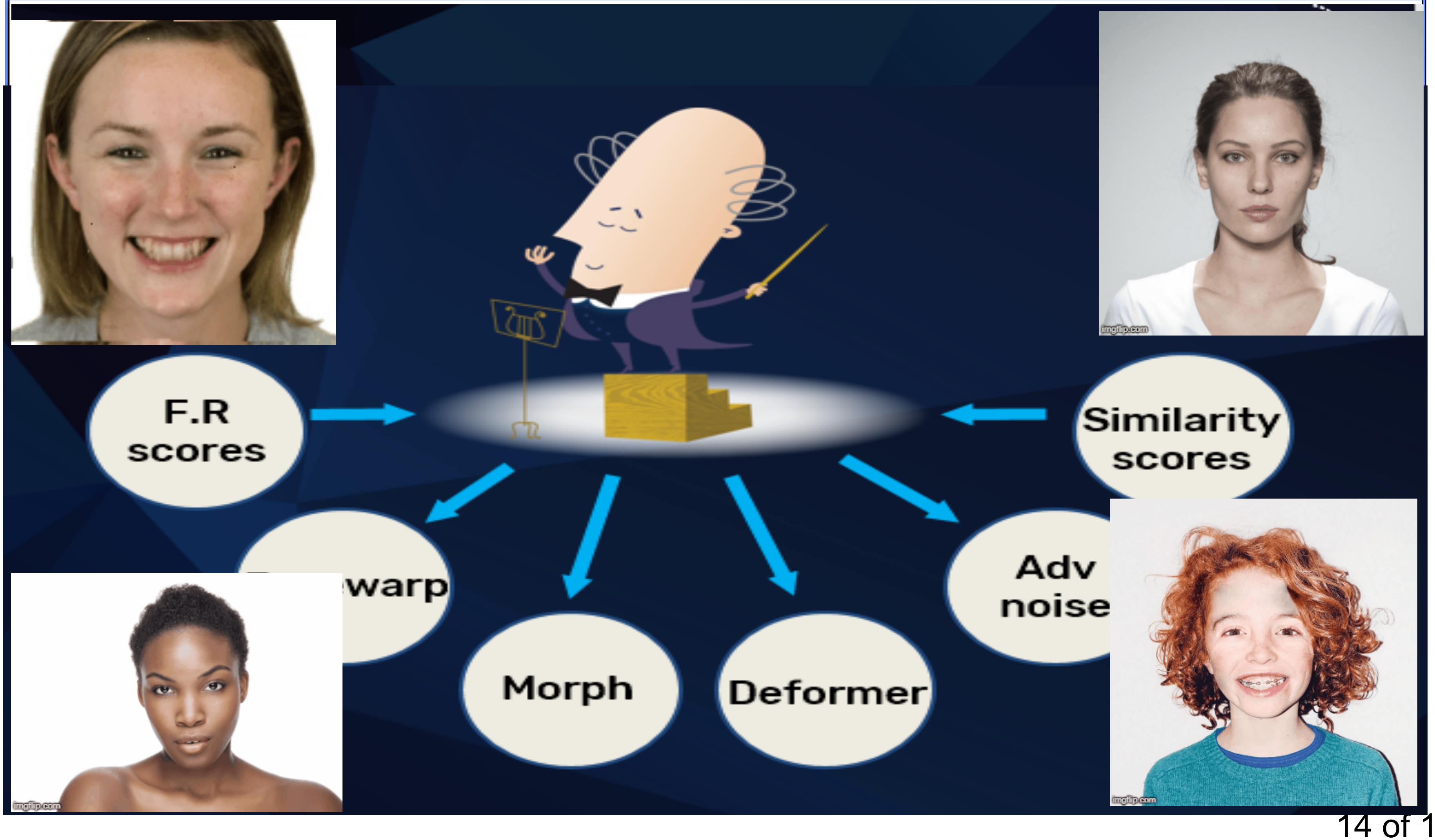
Signed Int ⌃ big ⌃ (select some data) ⊖ ⊕

0 out of 26385 bytes

Classic methods such as encryption, pixelation and blurring limit the use of the photo and does not fully protect against face recognition.



De-Identification



F.R scores

Similarity scores

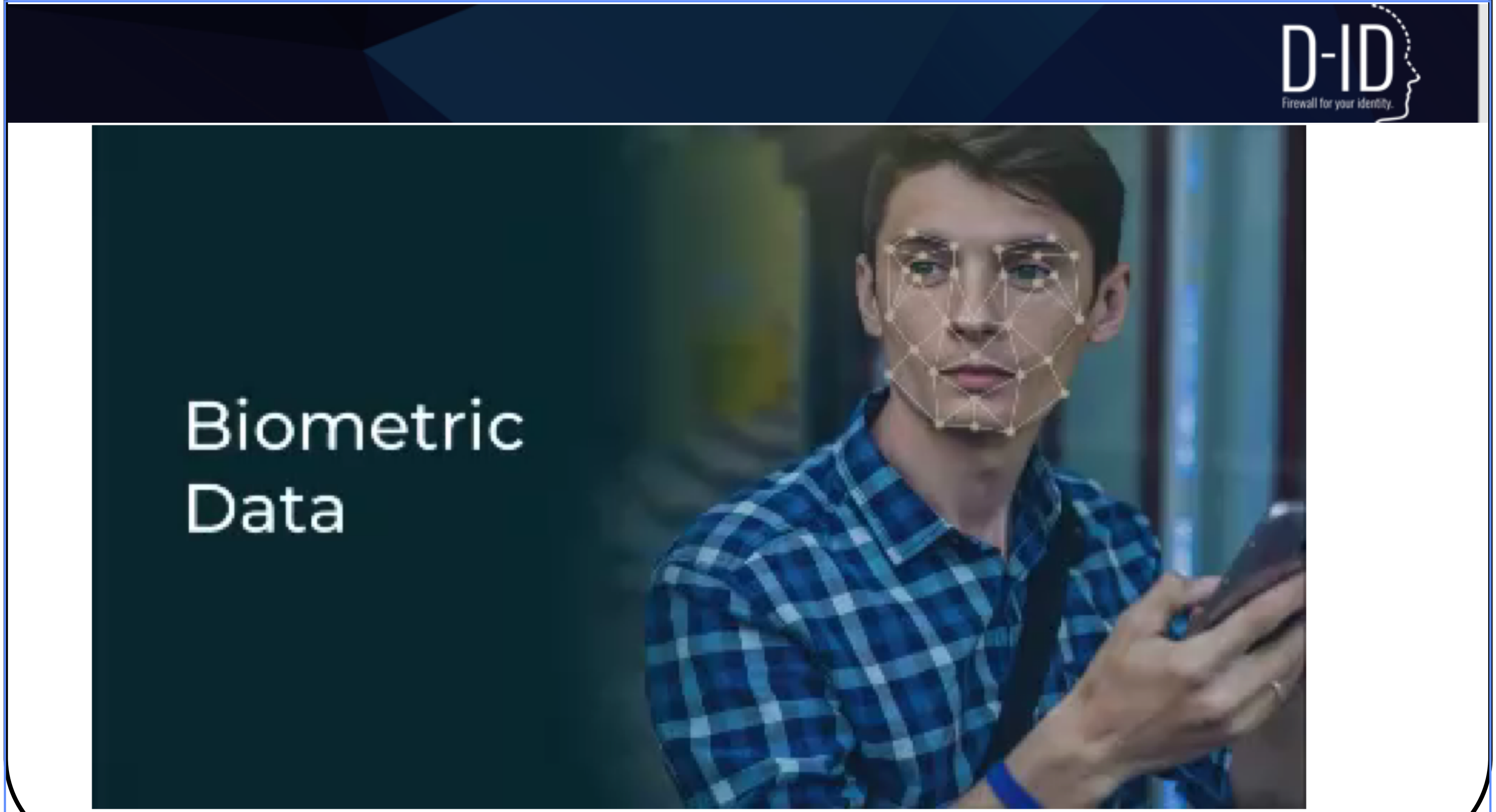
warp

Morph

Deformer

Adv noise

De-Identification



De-Identification - Usage

D-ID

Firewall for your identity.

Cloud Storage	**Social Networks**	**Financial Institutes**	**Health Care**	**Government & Security**

Summary

- Same as security – Privacy is a moving target – **an ever evolving challenge**
- Short stay could be a low privacy risk
- Low quality could be a low privacy risk
- Long time storage – hi risk -> encryption and de-identification

Final Summary

Mickey Cohen

Mickey@shanit.co.il +972-54-758-6312

Those wishing to receive their de-identified image may email.